After Action Reviews

Leveraging an AAR Process to Improve Compliance and Ethics Outcomes

The Ohio State University

The Ohio State University

Office of University Compliance and Integrity

Chris Glaros

Associate Vice President, Compliance Operations and Investigations

Glaros.3@osu.edu

Jessica Tobias

Ethics Director and Compliance Investigator

Tobias.80@osu.edu

“Success is a lousy teacher. It seduces smart people into thinking they can’t lose.”

Bill Gates

“The only real mistake is the one from which we learn nothing.”

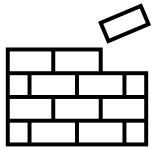
Henry Ford

How often do we end up solving the same problem over and over again?

How often do we have difficulty identifying who is responsible for solving such problems?

How often do we get exhausted and just want to move on after a long proactive or reactive initiative ?

What are the problems we're trying to solve?



A culture that is resistant to change

Systemic change is often very difficult in higher education

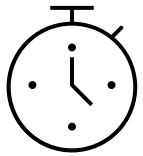
A bias towards individual accountability

We too often look for people to blame rather than seeking systemic solutions

A negative bias

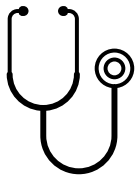
When issues arise, we tend to look for the negative rather than any positives

What are the consequences of not addressing these problems?



Repetitive problems

These same issues keep coming up time and again



Difficulty generalizing

We are unable to generalize from specific issues to broader solutions

Lack of traction

We fail to identify positive outliers that make change easier to drive and we fail to identify systemic opportunities

Relevant regulatory requirements

U.S. Department of Justice, Criminal Division:

> Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Evaluation of Corporate Compliance Programs, published in September 2024

Relevant regulatory requirements

The Department of Justice considers:

> the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned.

Evaluation of Corporate Compliance Programs, published in September 2024

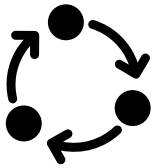
Our objectives, given these problems and requirements

- Develop and implement a consistent After Action Review (AAR) process to assess both proactive projects and reactive events
- Leverage AAR templates to scale evaluations for both small-scale, local actions and university-wide efforts
- Use AAR reporting to better evidence efficacy of compliance efforts

CrowdStrike was our catalyst

Worldwide financial damage estimated at least $10B

CrowdStrike distributed faulty software update that caused widespread problems with Windows computers

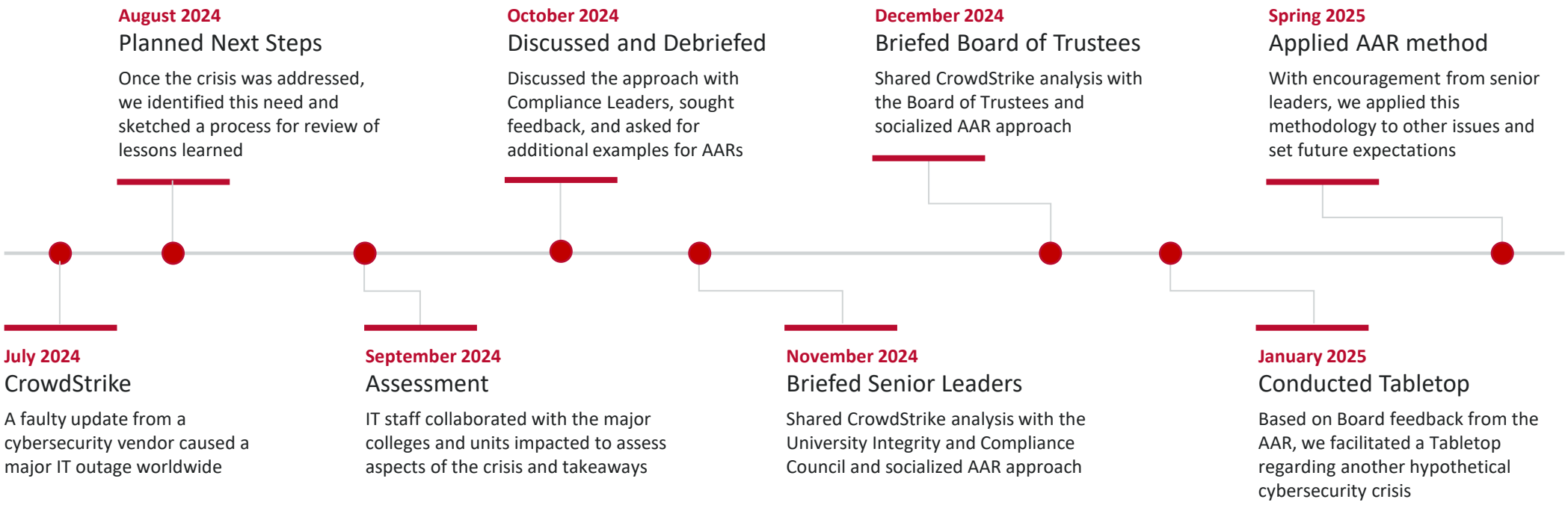


Distribution occurred automatically on July 19, 2024, between 12:00 and 1:30am to Windows hosts online and running the software

Approx. 8.5 million systems crashed and could not properly restart in “largest outage in the history of information technology”

Widespread outages occurred in businesses and governments worldwide (e.g., airlines, stock markets, emergency services)

Formalizing a process



July 2024
CrowdStrike
A faulty update from a cybersecurity vendor caused a major IT outage worldwide

August 2024
Planned Next Steps
Once the crisis was addressed, we identified this need and sketched a process for review of lessons learned

September 2024
Assessment
IT staff collaborated with the major colleges and units impacted to assess aspects of the crisis and takeaways

October 2024
Discussed and Debriefed
Discussed the approach with Compliance Leaders, sought feedback, and asked for additional examples for AARs

November 2024
Briefed Senior Leaders
Shared CrowdStrike analysis with the University Integrity and Compliance Council and socialized AAR approach

December 2024
Briefed Board of Trustees
Shared CrowdStrike analysis with the Board of Trustees and socialized AAR approach

January 2025
Conducted Tabletop
Based on Board feedback from the AAR, we facilitated a Tabletop regarding another hypothetical cybersecurity crisis

Spring 2025
Applied AAR method
With encouragement from senior leaders, we applied this methodology to other issues and set future expectations

After Action Review methodology

Process

- Common review template
- Collection of data and socialization of findings
- Leverage lessons of review to inform Board Cyber Incident Tabletop

Engagement

- **Key Central Units:** OTDI (Digital Security & Trust, Major Incident Manager & systems Support); OSU Wexner Medical Center (Clinical, IT, Security); Public Safety (Emergency Ops Center); Enterprise Risk Mgmt (Business Continuity); Facilities Operations and Development; Legal Affairs
- **Major Colleges/Other Units:** Athletics, Student Life, Arts & Sciences, Engineering, Advancement, Health Colleges, OH-Tech/OARnet

Analysis: Incident Response

OSU proved more resilient and recovered much more quickly than many other universities, state and local government, private sector orgs

Benefits of federated IT model

- **Diversity and distribution** of operating system platforms protected institution
- **Investment in security program** limited impact, substantially reduced duration of response & correction
- **Role clarity** learned from proactive efforts; local accountability reinforced initiative-taking
- **OTDI central oversight** provided consistency and assurance

Common approach

- **Prompt, consistent, prioritized decisions** facilitated by common risk language
- **Disaster Recovery** is mapped to Security & Risk framework and linked to NIST standards

Effective communications

- **All in on a common goal/pathway** during and after incident
- **Resilient communications** need multiple options for continuity
- **Relationships filled gaps:** when challenges occur, people fill in for others; expertise is shared as everyone knows common goals

Major Recommendations

Improve organizational flexibility through repeatable/documented processes

- **Formalize after action reviews** to better identify strengths and opportunities
- **Formalize linkages with existing notification processes** (e.g., OTDI P1 > Public Safety EOC > MC "code yellow")

Improve coordination of university-wide outages

- **Ensure consistency of all incident response processes** to improve overall resilience
- **Foster the four Cs**
  - **Communication:** Improve consistency and reliability of out-of-band communications
  - **Coordination:** Create single/shared Emergency Operations Center (EOC) for university-wide outages, with central CMDB/Asset Inventory
  - **Collaboration:** Improve linkage with Business Continuity; generate additional training for new processes and procedures created through After-Action Review
  - **Cooperation:** Align incident classifications & processes; clarify roles & communications channels between central to distributed units

Establish accountability and communications expectations

- Compliance Leaders to include AARs in their regular reports to our University Integrity and Compliance Council
    - Creates leadership familiarity with the concept and establishes expectation
- Legal Affairs and Compliance include AARs in reporting to the Board of Trustees
    - Demonstrates collaboration, critical analysis, and accountability for future challenges
- Continually debrief AARs done with Compliance Leaders
    - Improves our methodology, fosters collaboration, and instills confidence

Practice tips

- Develop the “Why” and clearly define the problems
- Envision success and work backwards from that outcome
- Draft a clear and flexible template
- Schedule appropriate time for meaningful conversations and analysis
- Make reporting easy and easy to understand
- Socialize the expectation that AARs happen regularly
- Show how AARs can help with both proactive and reactive issues

Potential challenges with AARs

- Legal liability
- Public Records
- Attorney-Client Privilege
- Time demands
- Friction with colleagues and partner units
- Misunderstandings from leadership
- Expectations for future success

Some other examples

After Action Review: Restructure of Internal Risk Governance

Summary

- Addressed need for rapid decision-making across diverse areas (e.g., NCAA, NIL, investigations, SA issues) and diverse constituents in an efficient and consistent manner

Institutional Impact

- Clarity of reporting structures and uniformity in risk rating
- Standardized communication with OLA, OUCI, FAR, and institutional leadership
- Consistency in outcomes for Athletics/BA decision-making

Analysis/Response

- Revised scope of Significant Matters Update meeting
- Creation of subgroups to manage NIL landscape, implementation of House case, and incorporation of BA initiatives/risks

Lessons Learned / Recommendations

- Importance of centralized and standardized internal risk management structure
- Broad-based communication of expectations surrounding earlier identification of initiatives and issues
- Collaboration across units with intersection of responsibilities and/or focus (i.e., NIL, revenue generation, etc.)

After Action Review: Privacy Incident Response

Summary

- Two privacy investigations involving multiple Medical Center departments (Human Resources, Compliance, Pharmacy, Nursing, Medical Center IT Security)

Institutional Impact

- Potential violation of the Privacy Rule
- Reputational

Analysis/Response

- Cross functional team collaboration
- Document sharing tools were helpful in accessing and keeping documents up to date
- Planned and proactively scheduled communication (daily meetings, designated Team Channel)

Lessons Learned / Recommendations

- Develop a data collection strategy early in the investigation
- Implement strategic pauses to re-align focus on privacy regulations
- Investigations revelated inconsistent issue response processes among various departments
- Led to a material change in our investigation process

After Action Review: Internal Audit of Youth Programs

Summary

- Youth protection compliance managed through a home-grown application.
- Functional, but highly manual processes. IA suggested exploring increasing automation functionality.

Institutional Impact

- Supervisors and unit leadership may be unaware of all youth programs in operation, or compliance status.
- Clunky, inefficient process for promoting full compliance (background checks, training, etc).

Analysis/Response

- Met with industry experts, compliance colleagues to identify best practices in automation.
- Process mapping for the lifecycle of youth programs (registration, compliance activities, through program operation/completion).

Lessons Learned /Recommendations

- Clearly identified processes to increase efficiency, leadership awareness and policy compliance.
- Increased compliance without costly staffing resources

After Action Review: Tragic Event at Graduation

Summary

- Mother of graduating student committed suicide by jumping from C-Deck of Ohio Stadium
- EHS Emergency Response team onsite and was called to initiate and coordinate the response

Institutional Impact

- Traumatizing for EHS staff who responded
- Event put a strain on EHS response team
- Unusual type of response for EHS; highlighted some gaps in our procedures

Analysis/Response

- Provided mental health resources to those who responded
- Reviewed response protocols as a team and with management to identify gaps and make recommendations for improvement

Lessons Learned /Recommendations

- **EHS did not have a plan for an extended response; there was no backup for original responders**
  - Changes made to response plans – EHS now has a primary and secondary responder for each week on call
  - If a response lasts more than 4 hours or if a response is unusually taxing, backup is called in to assist / relieve the primary responder
  - Clarified who decides when response is complete or grants approval for responder(s) to leave the scene (Director of Occupational Safety & Environmental Compliance)
- **Responders did not have access to food or water during the response, which lasted almost 12 hours**
  - Non-perishable snacks and bottled water have been added to the Emergency Response Vehicle

After Action Review:
Gainful Employment/Financial Value Transparency Requirements

Summary

- New reporting requirement for all Title IV eligible programs to ED: Enrollment, program and costs.
- ED to develop metrics such as high debt, low earning for programs and make publicly available (currently paused by ED)

Institutional Impact

- Broad impact for programs across university based on metrics assigned. Significant amount of data required over multiple years. Programs determined to be high debt/low earning face potential loss of financial aid.
- Public disclosures of metrics by ED and required institutional disclosures for programs depending on risk rating could have reputational and financial impacts.

Analysis/Response

- Created working group of stakeholders including: Financial Aid, Registrar, Enrollment Analytics, Research and Insights (EARI), Bursar, Systems and program contacts to prepare for data/reporting.
- Submitted initial data amidst changing guidance, delayed reporting requirements and deadlines.

Lessons Learned /Recommendations

- Collaboration and early preparation was key for complying with this requirement.
- Identified areas where reporting and data alignment could be improved to better track and prepare for additional requirements in the future. Currently pending additional guidance from ED.

Lessons Learned

- Reinforcement of need for AARs improved the ability to convert an individual issue to a systemic solution
- Units followed different AAR processes and inconsistently followed them
- AARs help identify the positive outcomes/practices that should be repeated or extended (“what we did right”)
- Alignment on a single AAR process improved cross-unit collaboration
- Demonstration of AAR results to leadership enabled compliance teams to evidence problem-solving capabilities
- Consistent use of the AAR approach reinforces the need for a “learning institution”
- Consistent use of the AAR approach reinforces a culture of values by reflecting positive learned outcomes

Your experiences and questions

Thank you!